JOURNAL OF ALGEBRA **202,** 229–242 (1998)
ARTICLE NO. JA977223

Testing Modules of Groups of Even Order for Simplicity*

Gerhard O. Michler†

Institut für Experimentelle Mathematik, Universität Essen-GH, Ellernstrasse 29, Essen, Germany

metadata, citation and similar papers at core.ac.uk

Øyvind Solberg‡

Department of Mathematical Sciences, NTNU, Lade, N-7055, Dragvoll, Norway

Communicated by Walter Feit

Received February 29, 1997

In this paper we exhibit an intimate relationship between the simplicity of an FG-module V of a finite group G generated by a noncentral involution $t \neq 1$ and some other element u in G and the socles of the eigenspaces E_λ for λ in $\{-1, 1\}$ of the involution t considered as FC-modules, where $C = C_G(t)$ is the centralizer of t in G. In fact the two main results yield new simplicity criteria for FG-modules V over fields F with odd or even characteristic p, respectively. For $p \neq 2$ the result follows from a general module theoretic simplicity test proved in the first section of the paper. It builds on ideas of the Meat-axe algorithm of previous work. We show the practicability of our new tests by examples. © 1998 Academic Press

INTRODUCTION

The main results of this article can be explained best for the special case of an n-dimensional FG-module M of a finite simple group G, where F is a commutative field of characteristic $p > 0$.

By the Feit–Thompson Theorem finite non-cyclic simple groups have even orders. Thus, by a well-known theorem of Brauer and Fowler [3] a

* The authors have been supported by the European TMR-project Contract CHRX-CT94-0601 and the DFG research project "Algorithmic Number Theory and Algebra."

† E-mail address: archiv@exp-math.uni-essen.de.
‡ E-mail address: oyvinso@math.ntnu.no.

0021-8693/98 $25.00

Copyright © 1998 by Academic Press
All rights of reproduction in any form reserved.

finite non-cyclic simple group G has an involution $t \neq 1$ for which the centralizer $C = G_G(t)$ has fairly large order, and for any such finite group C there exists at most a finite number of non-isomorphic simple groups G with an involution t such that $C_G(t) \cong C$. It is therefore reasonable to test the simplicity of a representation M of a simple group G by means of its restriction $M|_C$ to a centralizer $C = C_G(t)$ of an involution.

If $p \neq 2$, then the $n \times n$-matrix T of the involution t of G acting on the FG-module M has eigenvalues $\lambda = 1, -1$. The two eigenspaces E_λ of T in M are the solution spaces of the homogeneous linear equations $(T - \lambda I_n)x = 0$ for $x \in M$. Furthermore, as we note later (Proposition 1.3), it is entirely well known and obvious that E_{+1} and E_{-1} are FC-modules without common composition factors, such that $M|_C = E_{+1} \oplus E_{-1}$. In particular, we may choose one $\lambda \in \{1, -1\}$ such that

$$\dim_F E_\lambda = \min\{\dim_F E_{+1}, \dim_F E_{-1}\} \leq \tfrac{1}{2}\dim_F M.$$

In Theorem 3.1 it is shown that M is a simple FG-module if and only if $M = E_\lambda FG$, and the dual FG-module $M^* = ZFG$ for every simple FC-submodule Z of the dual FC-module E_λ^*.

In fact, Theorem 3.1 holds for finite perfect groups G with a non-central involution t such that $G = \langle u, t\rangle$ for some $u \in G$. It reduces the simplicity test for an FG-module M to the determination of $\operatorname{soc}(E_\lambda^*)$ and all the simple FC-submodules Z of $\operatorname{soc}(E_\lambda^*)$, where $\operatorname{soc}(X)$ denotes the socle of the module X. In the applications we assume this information to be known, because $\dim_F E_\lambda < \dim_F M$ and $|C| < |G|$.

For finite fields $F = GF(q)$ the precise number of these finitely many simple FC-submodules Z is given in Remark 3.2. It is only independent of the size of q when $\operatorname{soc}(E_\lambda^*)$ is multiplicity-free. If M is not simple, then at least one of the FG-submodules $E_\lambda FG$ of M or ZFG of M^* is proper, where Z is a simple FC-module in $\operatorname{soc}(E_\lambda^*)$ of E_λ^*. In any case a proper FG-submodule of M is constructed.

The proof of Theorem 3.1 is based on a general module theoretic simplicity test for finitely generated modules M over artin algebras Λ; see Proposition 1.1 stated in Section 1. It may be considered to be a ring theoretical generalization of the Holt–Rees simplicity test [6], which in turn builds on ideas of the Parker–Norton simplicity criterion [11].

In Section 2 we prove the relevant subsidiary results for perfect groups $G = \langle t, u\rangle$ generated by a non central involution t and some other element u. They imply that for fields F of odd characteristic p one only needs to consider the eigenspace E_λ of minimal dimension in the simplicity test given in Theorem 3.1.

In Section 4 we also prove an elementary simplicity test for finite groups G of even order with a noncentral involution t for finitely generated

FG-modules M over fields F what characteristic $p = 2$. Proposition 4.1 asserts that M is a simple FG-module if and only if $M = ZFG$ for all simple FC-submodules Z of $\mathrm{soc}(E_1)$, where E_1 is the eigenspace of t in $M|_C$ for the unique eigenvalue $\lambda = 1$.

We demonstrate the applicability of Theorem 3.1 and Proposition 4.1 by Examples 3.3 and 4.4, respectively. For $p = 2$ we consider the 782-dimensional irreducible representation of Fischer's simple group Fi_{23}. In this case the running time of our algorithm is about 20 seconds on an IBM RS6000/590. In each example the socle of E_λ and E_1, respectively, is a simple FC-module. So far we have not produced very efficient implementations of our simplicity tests. This will be done elsewhere, when we apply it to large representations of some sporadic simple groups.

Concerning our notation and terminology we refer to the books by Curtis and Reiner [5, 9].

The two authors gratefully acknowledge the computational assistance of H. Gollan. It is described in the examples. Furthermore, we thank the referee for several helpful suggestions concerning the presentation of this article.

1. A MODULE THEORETIC SIMPLICITY TEST

Using some ideas of the Parker–Norton Meat-axe algorithm [11] we prove in this section a new simplicity criterion for finitely generated modules M over artin algebras Λ, consequently for finite dimensional algebras over a (commutative) field. For a finitely generated right module M over an artin algebra Λ or finite dimensional algebra Λ over a field F denote by M^* the dual of M, which is a left module over Λ. In the latter case $M^* = \mathrm{Hom}_F(M, F)$. Our simplicity test for a right Λ-module M consists of a reduction technique, because we assume that for some proper subalgebra Γ of Λ we know a decomposition of the restriction $M_\Gamma = M' \oplus M''$ and that we can determine the socle of $(M')^*$ (over Γ).

PROPOSITION 1.1. *Let Λ be an artin R-algebra and Γ an R-subalgebra of Λ, where R is a commutative artin ring. Let M be a finitely generated right Λ-module. Suppose that the restriction M_Γ of M to Γ has a decomposition*

$$M_\Gamma = M' \oplus M''$$

such that no composition factor T of the head $M'/M'J$ of M' is isomorphic to a composition factor of the right Γ-module M'', where $J = J(\Gamma)$ denotes the Jacobson radical of Γ.

Then M is a simple Λ-module if and only if the following two conditions are satisfied:

(i) $M = M'\Lambda$.

(ii) $M^* = \Lambda Z$ *for each simple* Γ-*submodule* Z *of the left* Γ-*module* $(M')^*$.

Proof. If M is a simple Λ-module, then the conditions (a) and (b) of the proposition follows immediately. It remains to show the converse.

Suppose that M is not a simple Λ-module. Let L be a proper Λ-submodule of M.

First assume that M/L as a Γ-module does not have any of the simple Γ-modules T of $M'/M'J$ in its head. Let $i : M' \to M$ be the natural inclusion and let $\pi : M \to M/L$ be the natural projection. Since the simple modules T of $M'/M'J$ do not occur in the head of M/L, it follows that the image of M' under $\pi \circ i$ is contained in $(M/L)J = (MJ + L)/L$. Hence M' is contained in $MJ + L$. We have that $MJ = M'J \oplus M''J$, so that by induction we obtain that M' is contained in $M'J^j + M''J + L$ for all $j \geq 1$. Hence M' is contained in $M''J + L$. Replacing M by $M''J + L$ and observing that $(M''J + L)/L$ is isomorphic to a factor module of $M''J$, and therefore does not have any of the simple modules T of $M'/M'J$ as a composition factor, it follows by induction that M' is contained in L. Hence $M'\Lambda \subset L$, a contradiction to (i).

Now assume that M/L as a Γ-module does have one of the simple Γ-modules T of $M'/M'J$ in its head. Then T^* is contained in $(M/L)^*$, which is contained in $M^* = (M') \oplus (M'')^*$. The image of T^* in M^* is contained in $(M')^*$, because T^* is not isomorphic to any compostion factor of $(M'')^*$. Therefore the image of $(M/L)^*$ in M^* must contain a simple submodule S isomorphic to T^*. Therefore ΛS is contained in $(M/L)^*$, a proper Λ-submodule of M^*. This contradiction to condition (ii) completes the proof of the proposition. ▮

For finite dimensional algebras over a finite field $F = GF(q)$ we can give the exact number of the different embeddings of a simple module S in a direct sum S^d for an integer $d \geq 1$. This gives a practical limit on how large the multiplicities of the simples one can handle in practical computations.

PROPOSITION 1.2. *Let $M = S^d$ be a homogeneous semisimple Λ-module over the finite-dimensional algebra Λ over the finite field $F = GF(q)$ such that $F = \mathrm{End}_\Lambda(S)$ for the simple Λ-module S. Then there are $(q^d - 1)/(q - 1)$ different simple Λ-submodules of M.*

Proof. Since the Jacobson radical $J(\Lambda)$ of Λ operates trivially on M, we may assume that $\Lambda = \overline{\Lambda} = \Lambda/J(\Lambda)$. As M is homogeneous only the block of Λ containing S acts non-trivially on M. Hence we may assume that Λ is a simple F-algebra, i.e., $\Lambda \cong \mathrm{Mat}(n, F)$, where $n = \dim_F S$. Let $R = \mathrm{End}_\Lambda(M)$. As $F = \mathrm{End}_\Lambda(S)$, we have $R \cong \mathrm{Mat}(d, F)$. In particular, all three F-algebras Λ, R, and F are Morita equivalent. Therefore each simple Λ-submodule W of M corresponds uniquely to a 1-dimensional subspace W' of the F-vector space $V = F^d$. It is easy to see that there are $(q^d - 1)/(q - 1)$ one-dimensional subspaces in V. Hence the proof of the proposition is complete. ∎

The problem in applying the above simplicity test is to find a decomposition satisfying the assumptions. A situation where one has such a decomposition, occurs for groups rings FG of finite groups G with a noncentral involution over a field F with characteristic $p \neq 2$.

PROPOSITION 1.3. *Let G be a finite group of even order with a noncentral involution t with centralizer $C = C_G(t)$. Let V be an n-dimensional representation of G over a field F of characteristic $p > 0$. Let T in $\mathrm{GL}(n, F)$ be the matrix of t with respect to a fixed basis of V. For each eigenvalue λ in $\{-1, 1\}$ of T let E_λ be the eigenspace of T with respect to λ. Then the following assertions hold*:

(a) *Each E_λ is an FC-submodule of V. If $p \neq 2$, then $V|_C = E_{+1} \oplus E_{-1}$ and the two FC-modules E_{+1} and E_{-1} have no common composition factors.*

(b) *Every nonzero simple FG-submodule U of V contains a nonzero simple FC-submodule W_λ of E_λ for at least one λ, and $U = W_\lambda FG$.*

(c) *The representation V is a simple FG-module if and only if $V = SFG$ for all simple FC-submodules S of E_{+1} and E_{-1}.*

Proof. (a) This is obvious and well known.

(b) Let $U \neq 0$ be a nonzero FG-submodule of V, and $0 \neq v \in U$. Then either $w = v + Tv \neq 0$ or $Tv = -v$. Hence $0 \neq w \in E_{+1}$ or $0 \neq v \in E_{-1}$. In any case $U \cap E_\lambda$ is a nonzero FC-submodule for at least one $\lambda \in \{+1, -1\}$. Therefore it contains a nonzero simple FC-submodule W_λ of E_λ, because E_λ is a finite-dimensional FC-module. Hence $U = W_\lambda FG$ if U is a simple FG-submodule.

(c) The statement in (c) is an immediate consequence of (b). ∎

2. $(2, k)$-GENERATED GROUPS

Now we restrict ourselves to the situation where $G = \langle u, t \rangle$ with t being an involution. This hypothesis is satisfied by all alternating and sporadic finite simple groups, see [1]. As in Proposition 1.3 let V be an n-dimensional representation of V over a field F, and let U and T be the matrices of u and t in $\mathrm{GL}(n, F)$ with respect to a fixed F-basis of V. Let E_λ denote the eigenspace of T of an eigenvalue λ in $\{-1, 1\}$. This notation is used throughout this section.

First we find a sufficient condition for the representation V of G to have a nonzero intersection with the eigenspaces E_λ.

LEMMA 2.1. *If*

$$K_\lambda = \bigcap_{i=1}^{o(U)-1} \mathrm{Ker}(TU^i - U^iT)|_{E_\lambda} = \bigcap_{i=1}^{o(U)-1} \mathrm{Ker}(TU^i - \lambda U^i)|_{E_\lambda} = (0),$$

then any FG-submodule of V contains an eigenvector of T with eigenvalue $-\lambda$. Otherwise $\langle U^i(v)\rangle_{i=0}^{o(U)-1}$ is a nonzero FG-submodule of V for all nonzero v in K_λ.

Proof. Let W be an FG-submodule of V and w a nonzero element in W. If $w' = w - \lambda T(w)$ is nonzero, then

$$T(w') = \lambda^2 T(w) - \lambda T(w) = -\lambda(w - \lambda T(w)) = -\lambda w'$$

and the first claim holds in this case.

If $w' = 0$, then $T(w) = \lambda w$, hence w is in E_λ. By assumption there exists i_0 in $\{1, \dots, o(U) - 1\}$ such that $z = (TU^{i_o} - \lambda U^{i_o})(w)$ is nonzero. Then $T(z) = -\lambda z$ with z in $W \cap E_\lambda$, and therefore the first claim is also true in this case.

Suppose $K_\lambda \neq (0)$ and let v be nonzero in K_λ. Then v is in E_λ, and $TU^i(v) = \lambda U^i(v)$ for all i in $\{0, \dots, o(U) - 1\}$. Hence $M = \langle U^i(v)\rangle_{i=0}^{o(U)-1}$ is a nonzero FG = submodule of V. ∎

In the next two results we further investigate the role of the vector spaces K_{+1} and K_{-1} introduced above.

PROPOSITION 2.2. *If* char $F \neq 2$ *and* $K_{-1} \neq (0)$, *then G is not a perfect group.*

Proof. Since F contains the eigenvalues of T, the condition $K_{-1} \neq (0)$ is preserved by field extensions. So we may assume that F also contains the eigenvalues of U.

Let v be a nonzero element in K_{-1}. Then $TU^i(v) = -U^i(v) = U^iT(v)$ for $i = 0, 1, \dots, o(U) - 1$, because v is in E_{-1}. Hence v is in $\bigcap_{i=1}^{o(U)-1} \mathrm{Ker}(TU^i - U^iT)$. Therefore U and T have a common eigenvector w in E_{-1} over F by [10, Proposition 2.2]. Thus there is a nontrivial homomorphism of G into the multiplicative group F^* of F. Therefore the commutator subgroup G' of G is a proper subgroup, and G is not a perfect group. ∎

PROPOSITION 2.3. *If $K_1 \neq (0)$ and G is perfect, then K_1 is a trivial FG-submodule of V. In particular,* soc V *contains* 1_{FG}.

Proof. Since F contains the eigenvalues of T, the condition $K_1 \neq 0$ is preserved by field extensions. So we may assume that F is a splitting field for G.

Let $v \neq 0$ be an element of K_1. Then

$$TU^i(v) = U^i(v) = U^iT(v)$$

for $i = 1, 2, \ldots, o(U) - 1$, because $v \in E_1$ by Lemma 2.1. Hence G operates on the FG-submodule K_1 of V like the cyclic group $\langle U \rangle$. As G is perfect, this action is trivial. Therefore K_1 is a trivial FG-submodule of V.

In particular, soc(V) contains 1_{FG}. ∎

As an immediate corollary of these two propositions and Lemma 2.1 we have the following.

COROLLARY 2.4. *Let $G = \langle u, t \rangle$ with t being an involution. Let V be an n-dimensional FG-module with* $\mathrm{Hom}_{FG}(1_{FG}, V) = (0)$. *If G is a perfect group, then the following assertions hold*:

(a) $K_1 = (0)$ *and* $K_{-1} = (0)$.

(b) *For each λ in $\{-1, 1\}$ every simple FG-submodule W of V contains a nonzero eigenvector u_λ of T with eigenvalue λ.*

3. A SIMPLICITY TEST FOR GROUPS OF EVEN ORDER, $p \neq 2$

Using the subsidiary results of the previous sections we can now prove our main result.

THEOREM 3.1. *Let G be a finite perfect group with an involution t such that $G = \langle u, t \rangle$ for some u in G. Let $C = C_G(t)$ be the centralizer of t in G. Let F be a finite field of odd characteristic p and let V be an FG-module. If the trivial FG-module is not contained in* soc(V), *then the following assertions hold*:

(a) $V|_C = E_{+1} \oplus E_{-1}$, *and $E_\lambda \neq (0)$ for each $\lambda \in \{1, -1\}$ where E_λ denotes the eigenspace of t with respect to λ.*

(b) *V is a simple FG-submodule if and only if for some $\lambda \in \{1, -1\}$ the following two conditions are satisfied*:

(i) $V = E_\lambda FG$.

(ii) $V^* = ZFG$ *for every simple FC-submodule Z of E_λ^*.*

In fact, in (b), $\lambda \in \{1, -1\}$ *can always be chosen such that*

$$\dim_F E_\lambda = \min\{\dim_F E_{+1}, \dim_F E_{-1}\} \leq \tfrac{1}{2}\dim_F V.$$

Proof. We first note that t is a noncentral involution, because $G = \langle u, t \rangle$ is perfect.

(a) By Proposition 1.3(a) we have that $V|_C = E_{+1} \oplus E_{-1}$. Furthermore, $E_\lambda \neq (0)$ for each $\lambda \in \{1, -1\}$ by Corollary 2.4(b).

(b) Another application of Proposition 1.3(a) yields that the two FC-submodules E_{+1} and E_{-1} have no common composition factor. Now Proposition 1.1 completes the proof. ∎

Remark 3.2. Keeping the notation of Theorem 3.1, suppose that the socle of the FC-module E_λ^* has the direct decomposition $\operatorname{soc}(E_\lambda^*) = \bigoplus_{i=1}^k H_i$ into is homogeneous components $H_i = Z_i^{d_i}$ for $1 \leq i \leq k$, where Z_i is a simple FC-module. If the finite field $F = GF(q)$ has $q = p^r$ elements, then the number of spin calculations ZFG done in condition (b) (ii) of Theorem 3.1 equals

$$\sum_{i=1}^{k} \frac{q^{d_i} - 1}{q - 1}$$

by Proposition 1.2. Therefore, the simplicity test of Theorem 3.1 is computationally effective only for those FG-modules V for which all the multiplicities d_i of the simple composition factors Z_i of $\operatorname{soc}(E_\lambda)$ of the eigenspace E_λ are small.

In particular, this test works best if all $d_i = 1$. In this case the number of steps is even independent of the size q of the finite field.

The verification of the conditions of the simplicity criterion 3.1 is now illustrated for an 11-modular representation of the first sporadic Janko group.

EXAMPLE 3.3. Let G be the subgroup of GL(7, 11) generated by the two matrices

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$B = \begin{pmatrix} -3 & 2 & -1 & -1 & -3 & -1 & -3 \\ -2 & 1 & 1 & 3 & 1 & 3 & 3 \\ -1 & -1 & -3 & -1 & -3 & -3 & 2 \\ -1 & -3 & -1 & -3 & -3 & 2 & -1 \\ -3 & -1 & -3 & -3 & 2 & -1 & -1 \\ 1 & 3 & 3 & -2 & 1 & 1 & 3 \\ 3 & 3 & -2 & 1 & 1 & 3 & 1 \end{pmatrix}.$$

Then by Janko [7], $G = \langle A, B \rangle$ is simple group with order $|G| = 175560$. The following element $T = (AB)^5$ is an involution

$$T = \begin{pmatrix} 5 & 0 & 0 & 0 & -2 & 4 & 0 \\ 0 & 2 & -3 & 1 & 0 & 0 & 3 \\ 0 & -3 & 3 & -1 & 0 & 0 & -2 \\ 0 & 1 & -1 & 3 & 0 & 0 & 1 \\ -2 & 0 & 0 & 0 & -4 & -5 & 0 \\ 4 & 0 & 0 & 0 & -5 & -2 & 0 \\ 0 & 3 & -2 & 1 & 0 & 0 & 3 \end{pmatrix}$$

and the element $U = AB^{-1}$ has order 19.

$$U = \begin{pmatrix} 2 & 1 & -1 & -3 & -1 & 3 & 3 \\ -1 & 1 & -3 & -1 & -3 & 3 & -2 \\ -1 & 3 & -1 & -3 & -3 & -2 & 1 \\ -3 & 1 & -3 & -3 & 2 & 1 & 1 \\ -1 & 3 & -3 & 2 & -1 & 1 & 3 \\ -3 & 3 & 2 & -1 & -1 & 3 & 1 \\ -3 & -2 & -1 & -1 & -3 & 1 & 3 \end{pmatrix}$$

The following two elements generate the centralizer $C = C_G(T) \cong \langle T \rangle \times \mathrm{PSL}(2,5)$ of T in G:

$$X = \begin{pmatrix} -2 & 1 & 1 & 3 & 1 & 3 & 3 \\ 1 & 1 & 3 & 1 & 3 & 3 & -2 \\ 1 & 3 & 1 & 3 & 3 & -2 & 1 \\ 3 & 1 & 3 & 3 & -2 & 1 & 1 \\ 1 & 3 & 3 & -2 & 1 & 1 & 3 \\ 3 & 3 & -2 & 1 & 1 & 3 & 1 \\ 3 & -2 & 1 & 1 & 3 & 1 & 3 \end{pmatrix}$$

$$Y = \begin{pmatrix} 3 & 1 & -4 & -5 & -2 & 3 & 5 \\ 5 & -3 & 5 & -1 & 0 & 5 & 2 \\ 2 & 1 & 2 & 0 & -1 & 2 & 3 \\ -4 & 2 & 3 & -5 & -2 & 0 & 3 \\ -5 & 4 & -5 & 2 & 3 & -3 & 1 \\ -4 & 4 & 3 & -5 & -2 & -4 & 5 \\ 4 & -3 & 1 & 3 & -1 & 2 & -4 \end{pmatrix},$$

where X and Y have been constructed from T and U by H. Gollan as follows. Starting with the elements T and U, define

$$\begin{aligned}
T_0 &= T \\
T_1 &= U \\
T_2 &= T_0T_1^3T_0T_1^2T_0T_1^5T_0T_1^2T_0T_1^{-1}T_0T_1^{-1} \\
T_3 &= T_1^5T_0T_1^2T_0T_1T_0T_1^{-1}T_0T_1^{-5} \\
T_4 &= T_1^3T_0T_1^2T_0T_1^3T_0T_1T_0T_1^2T_0T_1^{-4}T_0T_1^{-2}T_0T_1^{-3}T_0 \\
T_5 &= T_4T_2^3T_2T_4^{-2}T_3^{-1}T_2^{-1} \\
T_6 &= T_4T_2T_3T_2T_4^{-1}T_3^{-1}T_2^{-1}.
\end{aligned}$$

Then we have $X = T_6T_2^3T_2^2T_0$, and $Y = T_6T_5^2T_3T_2$.

Since $C = C_G(T) = \langle X, Y\rangle \leq \langle T, U\rangle$, and $U \notin C$, we get $G = \langle T, U\rangle$ because C is a maximal subgroup of G by Janko's paper [7]. As T is a symmetric matrix of order 2, and the transpose U^T of U equals U^{-1}, it follows that $V = F^7$ is a self-dual FG-module over $F = GF(11)$.

As $Y \in \mathrm{PSL}(2,5)$, and $X_1 = XT \in \mathrm{PSL}(2,5)$ we obtain $\mathrm{PSL}(2,5) = \langle X_1, Y\rangle$.

The eigenspaces E_λ of T for $\lambda \in \{+1, -1\}$ on the 7-dimensional FG-module $V = F^7$ are $E_{+1} = \{v_1, v_1X_1, v_1Y\}$ with $v_1 = (0,0,1,0,0,0,1)$, $E_{-1} = \{v_2, v_2X_1, v_2Y, v_2Y^2\}$ with $v_2 = (0,9,10,0,0,0,1)$. Furthermore, $V = E_{+1} \oplus E_{-1}$. Since the simple $\mathrm{PSL}(2,5)$-modules over $F = GF(11)$ have dimensions $1, 3, 4$, and 5 by [4, p. 2], it follows immediately that E_{+1} is a simple $\mathrm{PSL}(2,5)$-module and therefore it is a 3-dimensional simple FC-module.

Let $u \cdot w$ be the scalar product of u and v in $V = F^7$, and $(E_{-1})^\perp = \{u \in V \mid u \cdot w = 0 \text{ for all } w \in E_{-1}\}$. Since T is a symmetric diagonalizable matrix over F, its eigenvectors corresponding to different eigenvalues are orthogonal. Hence $(E_{-1})^\perp = E_{+1}$ as F-vector spaces. Since $V \cong V^*$ as FC-modules, we have $E_{+1}^* = E_{+1}FC \leq V^*$ by [5, p. 411].

Now applying U to E_{+1} and E_{+1}^* we get that

$$V = \langle v_1, v_1X_1, v_1Y, v_1U, v_1X_1U, v_1YU, v_1U^2\rangle = E_{+1}FG,$$

and

$$V^* = \langle v_1, v_1X_1, v_1Y, v_1U^{-1}, v_1X_1U^{-1}, v_1YU^{-1}, v_1U^{-2}\rangle = E_{+1}^*FG.$$

Hence V is a simple FG-module by Theorem 3.1.

4. A SIMPLICITY TEST FOR GROUPS OF EVEN ORDER, $p = 2$

There is no analogous result of Theorem 3.1 for group representations V of finite groups G of even order over fields F with characteristic $p = 2$. However, Proposition 1.3(c) yields the following useful simplicity test.

PROPOSITION 4.1. *Let F be a field of characteristic 2. Let V be a finitely generated FG-module of a finite group G with a noncentral involution $t \neq 1$ and centralizer $C = C_G(t)$. Then $E_1 = \{v \in V \mid vt = v\}$ is an FC-module.*

Assume that $\operatorname{soc} E_1 = \bigoplus_{i=1}^{s} S_i^{d_i}$, where S_i are simple FC-modules with $S_i \not\cong S_j$ for $i \neq j$. Then V is a simple FG-module if and only if $SFG = V$ for all simple FG-submodules S of $S_i^{d_i}$ for all $i = 1, \ldots, s$.

Let R be a discrete rank one valuation ring with maximal ideal πR, residue class field $F = R/\pi R$ of characteristic $p > 0$, and quotient field S of characteristic zero. If F and S are splitting fields for the finite group G, then the triple (F, R, S) is called a p-modular splitting system for G.

An FG-module V is called *liftable*, if there is an RG-lattice X such that

$$X \otimes_R F = X/X\pi \cong V$$

as FG-modules.

The following result due to P. Landrock [8] gives a good lower bound for the dimension of the eigenspace E_1 of an involution $t \neq 1$ of G in a liftable FG-module V.

LEMMA 4.2. *Let (F, R, S) be a 2-modular splitting system for the finite group G with a noncentral involution $t \neq 1$. Let $V = X/X\pi$ be a liftable FG-module, and let χ be the complex character afforded by $X \otimes_R S$. If $E_1 = \{v \in V | vt = v\}$, then*

$$\dim_F E_1 \geq \tfrac{1}{2}\left[\dim_F V + |\chi(t)|\right].$$

Remark 4.3. Whenever V is a non-projective liftable FG-module, then $\chi(t) \neq 0$ for at least one involution t of G. Hence $\dim_F E_1 > \frac{1}{2}\dim_F V$ for such representations V of G and involutions $t \neq 1$.

Nevertheless, the following example shows that Corollary 4.1 is a practical simplicity test. Using the Norton−Parker Meat-axe algorithm [11] R.A. Wilson had proved before in [13] that the following FG-module V is simple.

EXAMPLE 4.4. Let G be the finite sporadic simple group Fi_{23} of Fischer of order $|G| = 2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$. By the Atlas [4, p. 177], G has an involution $t \neq 1$ with centralizer $C = C_G(t) \cong 2\mathrm{Fi}_{22}$, the 2-fold cover of the simple sporadic group $H = \mathrm{Fi}_{22}$ of Fischer.

Let (F, R, S) be a 2-modular splitting system for G. By the Atlas [4] the permutation SG-module $(1_C)^G$ splits into the irreducible SG-modules 1_G, $\hat{X}$ of dimension $\dim_S \hat{X} = 782$, and $\hat{Y}$ of dimension $\dim_S \hat{Y} = 30888$.

Let X be an RG-lattice of $\hat{X}$, and let $V = X \otimes_R F = X/X\pi$. Then V is a liftable FG-module of dimension $\dim_F V = 782$. Let $E_1 = \{v \in V \mid vt = v\}$ be the eigenspace of t in V, and let χ be the complex irreducible character of G afforded by $\hat{X} = X \otimes_R S$. Then $\chi(t) = 78$ by [4, p. 178]. Hence $\dim_F E_1 \geq \frac{1}{2}(782 + 78) = 430$ by Lemma 4.2. By Frobenius reciprocity we have

$$\chi|_C = 1_C + \chi_3 + \chi_{66},$$

where χ_3 and χ_{66} are the irreducible complex characters of H in the notation of [4, p. 156–157] of degrees $\chi_3(1) = 429$ and $\chi_{66}(1) = 352$. As all the values of the irreducible characters $\chi, 1_C, \chi_3$, and χ_{66} are rational, we see that V and V/E_1 are self-dual FG- and FC-modules, respectively. Since $\chi_{66}(t) = 0$, it follows from Landrock's proof [8] of Lemma 4.2 that $\dim_F E_1 = 430$.

Any R-form of χ_3 has 2-modular irreducible constituents of dimensions 1, 78, 350. Similarly, any R-form of χ_{66} has 2-modular irreducible constituents $I = 1_G$ with multiplicity 2 and 350.

Using Proposition 4.1 we now check that V is a simple FG-module. In [14] Wilson has given two matrices X and Y in $\mathrm{GL}(782, 2)$ generating the Fischer group G in representation corresponding to V. In the Atlas notation [4], X belongs to the conjugacy class $2B$ and Y to $3D$. Furthermore the element XY has order 28. Wilson [14] also gives two generators K and L of the centralizer $C = C_G(t)$ as follows. Let

$$D = (XY)^{13}\Big[\big((XY)^3Y\big)^2 XY\Big]^{13}(XY)^{-13},$$

$$L = (XY^2)^{11}\Big[\big((XY)^2Y\big)^2 XY\Big](XY^2)^{-11},$$

$$K = (DL)^{11}D.$$

Then $C = C_G(t) = \langle L, K\rangle$. Using these generators L and K, H. Gollan has found that the involution t of C can be represented by the matrix

$$T = (KL^2)^{21} \in \mathrm{GL}(782, 2).$$

By means of MAGMA [2] he has computed the eigenspace E_1 of T in V, and the socle series of this FC-module:

$$E_1|_C = \begin{array}{c} I \quad \oplus \quad 78 \\ 350 \\ I \end{array}$$

In particular, $\mathrm{soc}(E_1) = I$. Furthermore, a computer calculation with MAGMA shows that $V = \mathrm{soc}(E_1)FG = IFG$. Hence V is a simple FG-module by Proposition 4.1.

Remark 4.5. Example 4.4 was also used by H. Gollan to compare the algorithm stated in Proposition 4.1 with the Parker–Norton Meat-Axe algorithm. He used the Computer Algebra System MAGMA [2] and its implementations of representation theory algorithms. Since the Meat-Axe and the computation of the socle use probabilistic algorithms he did 25 test runs on an IBM RS6000/590 in each case. The following table shows on the left the timings for the MAGMA implementation of the Parker–Norton Meat-Axe, on the right of the total timings for the algorithm described in Proposition 4.1, i.e., computation of the eigenspace E_1, of the socle of E_1 as an FC-module, and of the spin $\mathrm{soc}(E_1)FG = V$. In each case the first row shows the average time of the 25 test runs in seconds. Rows 2 and 3 give the minimum and maximum time.

	Meat-Axe	Proposition 4.1
average	29, 79	19, 68
min.	19, 61	15, 18
max.	48, 14	24, 82

In the application of the algorithm stated in Proposition 4.1 the computation of a vector space for the eigenspace E_1 took only 0.74 seconds, and the time for the spin ZFG was 2.55 seconds. Thus the computation of $\mathrm{soc}(E_1)$ by means of MAGMA took most of the time.

REFERENCES

1. M. Aschbacher and R. Guralnick, Some applications of the first cohomology group, *J. Algebra* **90** (1984), 446–460.
2. W. Bosma and J. Cannon, "MAGMA Handbook," Sydney, 1993.
3. R. Brauer and K. Fowler, On groups of even order, *Ann. Math.* **62** (1965), 565–583.
4. J. H. Conway, R. T. Curtis, S. P. Norton, R. Parker, and R. A. Wilson, "Atlas of Finite Groups," Clarendon Press, Oxford, 1985.
5. C. W. Curtis and I. Reiner, "Representation Theory of Finite Groups and Associative Algebras," Wiley, New York, 1962.

6. D. F. Holt and S. Rees, Testing modules for irreducibility, *J. Austral. Math. Soc. Ser. A* **57** (1994), 1–16.
7. Z. Janko, A new finite simple group with abelian Sylow 2-subgroups and its characterization, *J. Algebra* **3** (1966), 147–186.
8. P. Landrock, On centralizers of *p*-elements in indecomposable modules, *Proc. Amer. Math. Soc.* **82** (1981), 325–329.
9. P. Landrock, ''Finite Group Algebras and Their Modules,'' Cambridge Univ. Press, Cambridge, 1983.
10. G. Michler, An algorithm for determining the simplicity of a modular group representation, *J. Symbolic Comput.* **6** (1988), 105–111.
11. R. Parker, The computer calculation of modular characters: The Meat-Axe, *in* ''Computational Group Theory,'' (M. Atkinson, Ed.), pp. 267–274, Academic Press, London, 1984.
12. M. Schönert and others, ''GAP-Groups, Algorithms, and Programming,'' Lehrstuhl D für Mathematik, RWTH, Aachen, Germany, 1992.
13. R. A. Wilson, A new construction of the Baby Monster and applications, *Bull. London Math. Soc.* **25** (1993), 431–437.
14. R. A. Wilson, Atlas of finite group representations, world wide web, http://www.mat.bham.ac.uk/ atlas.